Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

010.103 Change Control Policy

Version 2.3
July 24, 2019

Revision History

Date	Version	Description	Author
6/21/2007	1.0	Effective Date	CHFS IT Policies Team Charter
7/24/2019	2.3	Review Date	CHFS OATS Policy Charter Team
7/24/2019	2.3	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	7/24/2019	Jennifer L. Harp	
CHFS Chief Information Security Officer (or designee)	7/24/2019	DENNIS E. LEBER	

Table of Contents

1 Policy Definitions

- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State Law (Kentucky Revised Statute 61.878); Protected Health Information; Federal Tax Information; Social Security and Credit Card numbers.
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Data Classification:**
    - **NIST High Impact Level:** Defined by National Institute of Standards and Technology (NIST) 800-53 Revision 4 as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high: severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
    - **NIST Moderate Impact Level:** Defined by NIST 800-53 Revision 4 as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high; serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
    - **NIST Low Impact Level:** Defined by NIST 800-53 Revision 4 as an information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low; limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization's ability to carry out its mission, minor financial loss, and/or minor harm to individuals.
- **Dedicated Environments:** Defined by CHFS as dedicated Development and Test Environments that would have exclusive use of specific services provided on a server. A dedicated environment could have functionally related applications,

databases and report services.

- **Electronic Personal Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. The individually identifiable health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.
- **Personally Identifiable Information (PII):** Defined by Kentucky Revised Statute (KRS) Chapter 61 House Bill 5 (HB5) and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: All information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver's license numbers,

employee ID numbers, license plate numbers, and compensation information. The Commonwealth proprietary information including but not limited to intellectual property, financial data and more.

- **Shared Environments**: Defined by CHFS as any environment where non-related application, database, report, or other services for different application platforms (Development, Test, Training, and Production) are housed on the same server. Multiple applications hosted on the same server are also considered shared environments.
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS with final approval and appointment by the Kentucky Personnel Cabinet.
- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Application and Technology Services (OATS) must establish a comprehensive level of security controls through a change control policy. This document establishes the agency's Change Control Policy which helps manage risks and provides guidelines for security best practices regarding change control.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the NIST. Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

An individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) self-assessments through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

4 Policy Requirements

4.1 General Change Control

The Change Control Policy was implemented to establish unified control for changes to all servers. The Change Control Board (CCB) was established to ensure that the Change Control Policy is implemented and maintained as published. All data fixes shall be logged and recorded by the appropriate agency, and shall be auditable. CCB approval must be obtained for any data fix that requires a database restart or system reboot.

4.2 Description of Components

CHFS IT has implemented a change control process consisting of, but not limited to, an online change control portal, a weekly meeting with designated CCB, and an emergency approval contact list.

CHFS has a change control portal, Information Technology Management Portal (ITMP). This online portal is used for the purpose of submitting, reviewing, and monitoring all change controlled processes that have been established. The availability of this portal has been limited to technology personnel.

The CCB has the responsibility of managing all change control requests. This responsibility consists of the review, approval, denial and referral of such requests. The CCB shall consist of at least one representative of each affected branch within OATS. The CCB shall meet weekly at a designated and published time (this can be by conference call.) The CCB does not possess the responsibility to verify the technical feasibility of requested changes; this responsibility falls on the requestor or requestor's designee. The CCB does not replace, or act in lieu of, management approval. All requests must be planned and cleared by all normal internal processes before a change control request is submitted.

Emergency approval designees hold the responsibility for approving all requests deemed an emergency. This shall consist of a primary and a secondary contact. There is an expectation that such requests should receive a response within three (3) hours. If there is an occasion when no response is received for an emergency request within three hours, the request should be forwarded to the CCB Chairperson and/or upper level executive management.

4.3 Change Control Process: Production and Training Systems Environment

Hardware, Operating System, System Restarts Application, or other Production System changes without the submission and prior approval of the standard Change Control Request process.

All CCB approved requests must be submitted to the Commonwealth Office of Technology's (COT) Change Advisory Board (CAB) for final approval and action.

4.4 Change Control Process: Development and Test Systems Environment

Dedicated Development and Test Environments have exclusive use of specific services provided on a server. All changes to non-production, except Development, (application modifications, database modifications, etc.) shall be entered into the ITMP change control portal for documentation purposes only. Lower environment change controls do not require CCB approval.

For Shared Development and Test Environments, no change concerning any modification of hardware, operating systems, installation of new applications, databases (i.e. SQL, Oracle), or system restarts shall be applied to a non-production, shared system without the submission and prior approval of a change control request to the CCB. All other changes (application modifications, database modifications, etc.) shall be entered into the change control portal for documentation purposes only.

4.5 Request Submission

All testing, planning, notification and management approval must be completed prior to submitting a change control request. Upon submission, all requests must be completed as fully as possible. Failure to complete a required task, provide proper, adequate or required information may result in the denial or delay of the change request.

Change requests must be submitted in a timely manner. All non-emergency requests shall be reviewed weekly during the regularly scheduled change control meeting. All requests received after 10:00 am, the morning of the scheduled meeting, shall be reviewed during the following week's CCB meeting.

Careful evaluation must be applied to the following areas when submitting a change control request:

Risk Factor Level	Risk Factor Description
Minimum	Little to no impact of current services
Medium	Clear and noticeable impact of services
Severe	Significant impact on the services and the business. Considerable manpower and/or resources needed.

Impact Level	Impact Description
Low	Change leads to minor improvement
Medium	Change will solve irritating errors or missing functionality
High	Change needed as soon as possible (Potentially damaging)
Emergency	Change necessary now (Otherwise severe business impact) *May not be applicable to scenarios that could have/should have been planned

Submission of a request shall be assigned to the next change control meeting, at which time the CCB will review, verify scheduling and assess project impact of the request. The requestor will be notified of the CCB decision.

Upon approval from the CCB, the requestor may proceed with the noted changes. Should there be any modifications to the request, it will be postponed and re-submission will be required. Upon denial of a request, all intended operations must be stopped. The requestor may review the denial comments from the CCB and resubmit accordingly.
If there is a change of status for any request, including completion of tasks, it is the requestor's responsibility to review and update the request. Prior to CCB approval, the requestor should submit their request to the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov) to open a ticket. If a vendor is completing the

release, the ticket will be used either for assistance or information. If available, all requests should include documentation with release instructions.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Procedure: COT-009- Change Management Procedure
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- Information Technology Management Portal (ITMP)
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information